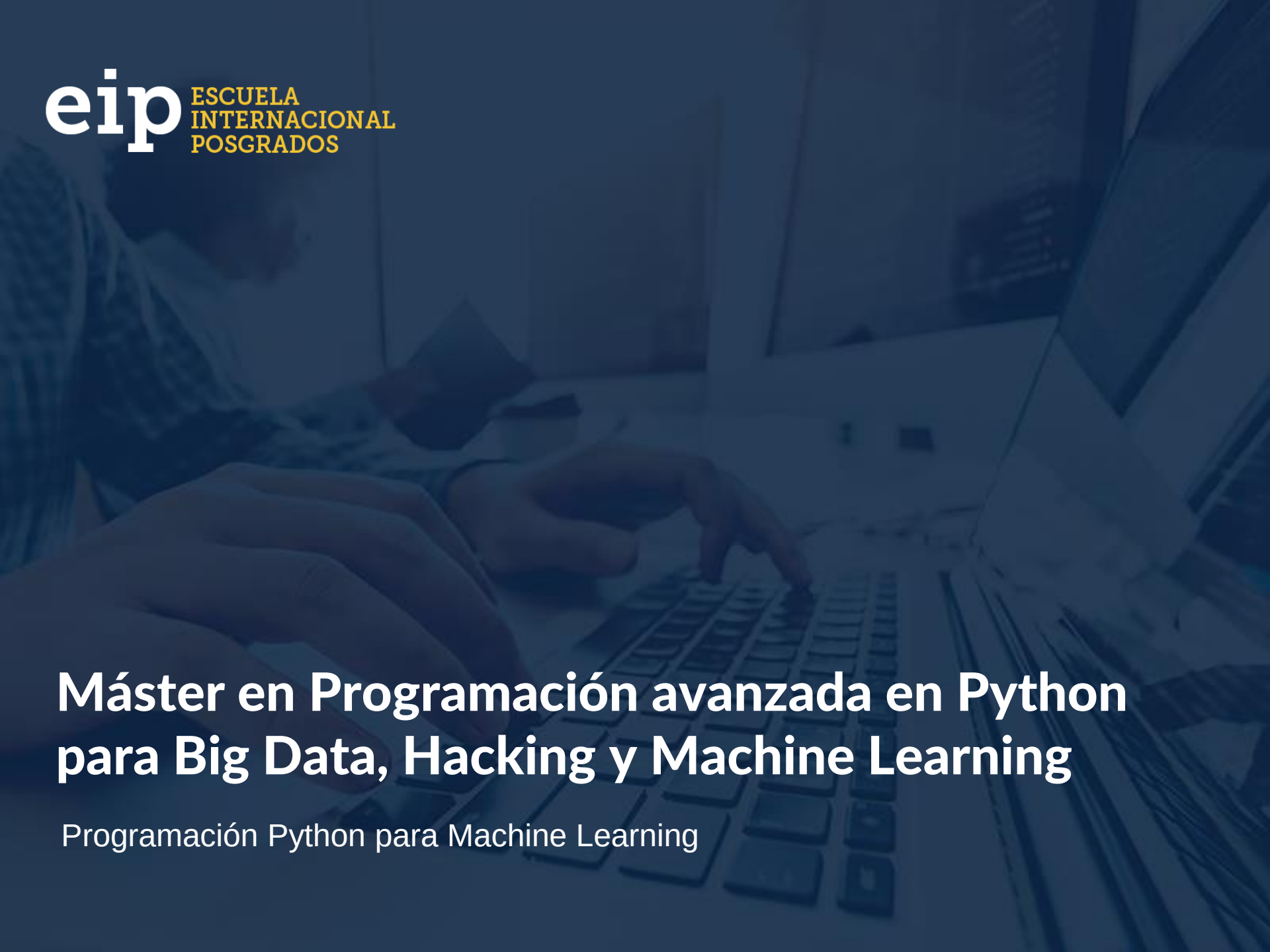

eip ESCUELA INTERNACIONAL POSGRADOS

Máster en Programación avanzada en Python para Big Data, Hacking y Machine Learning

Programación Python para Machine Learning

MÓDULO 01

OSINT con Python y recolección de información activa.

Recolección de información en fuentes abiertas.

La proliferación de servicios en línea y el aumento de usuarios en Internet han dado como resultado una enorme cantidad de información pública de todo tipo. Las técnicas utilizadas para recolectar y procesar dicha información son conocidas como OSINT (Open Source Intelligence)

Las redes sociales, blogs, información disponible en sitios de indexado y los búscadores especializados representan un medio muy útil para ingenieros sociales y atacantes.

Las técnicas OSINT entran en el marco de la ciberinteligencia y pueden ser útiles para cuestiones generales como conocer la reputación de una persona o la evaluación de tendencias de mercados para la elaboración de estudios sociológicos/psicológicos.

Consultas WHOIS

WHOIS es un protocolo que permite realizar consultas sobre dominios y direcciones.

Los servidores whois contienen información que se replica entre varios nodos en la red para proporcionar acceso distribuido a dicha información.

Los datos que almacena un servidor whois sobre un dominio pueden contener detalles como el nombre completo del propietario del dominio, teléfonos y direcciones etc. Opcionalmente, el propietario del dominio puede hacer que dichos registros sean privados.

Consultas DNS

DNS es un protocolo de texto basado en UDP que permite resolver nombres de dominios a direcciones IP y viceversa.

Esencialmente, los ordenadores se comunican entre ellos por medio de direcciones MAC/IP (dependiendo de la capa en el modelo OSI), dado que dichas direcciones pueden ser difíciles de recordar, el protocolo DNS permite la asociación de nombres con direcciones para que sean fáciles de recordar.

Existen registros para direcciones IPv4, IPv6, Nameservers, servidores de correo, etc.

La estructura de un servidor DNS es la de una base de datos jerárquica, por este motivo es necesario realizar consultas para navegar por los registros.

Se trata de un sistema que provee una capa de abstracción muy conveniente para los usuarios, ya que las direcciones IP pueden cambiar sin que esto suponga cambio alguno en el dominio, algo que facilita enormemente la gestión de servidores.

Recolección de información en fuentes abiertas: Shodan.

Shodan es un motor que funciona de un modo muy similar a los buscadores en Internet, con la diferencia de que no indexa los contenidos de los servidores encontrados, sino las cabeceras y banners devueltos por los servicios.

Es conocido como "el google de los hackers" ya que permite realizar búsquedas aplicando diferentes tipos de filtros para recuperar servidores que utilicen un protocolo concreto.

Actualmente, soporta servicios como HTTP/HTTPS, SSH, FTP, Telnet, SNMP y SIP.

Para utilizar Shodan programáticamente es necesario tener una cuenta en Shodan con una “Developer Shodan Key”.

Integración Python y Nmap

Nmap es un potente escáner que permite no solamente permite detectar los puertos abiertos de un sistema o segmento de red, sino que también permite realizar operaciones avanzadas para recolectar información sobre un objetivo y detectar vulnerabilidades.

Python-nmap es una librería que utiliza nmap desde cualquier script escrito en Python, algo que puede ser muy útil para optimizar tareas de descubrimiento y análisis de objetivos.

Es posible utilizar python-nmap para atacar múltiples objetivos de forma asíncrona

MUCHAS GRACIAS POR SU ATENCIÓN

eip ESCUELA INTERNACIONAL POSGRADOS


decheverri@grupomainjobs.com


Daniel Echeverri
https://www.linkedin.com/in/adastra1/


twitter.com/eiposgrados


facebook.com/eiposgrados


instagram.com/eiposgrados